Apache RocketMQ Command Execution Vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-33246
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-24 15:15:00 UTC
Updated	2023-07-12 12:15:00 UTC
Description	For RocketMQ versions 5.1.0 and below, under certain conditions, there is a risk of remote command execution. Several c

Risk And Classification

EPSS: 0.943880000 probability, percentile 0.999720000 (date 2026-05-11)

CISA KEV: Listed on 2023-09-06; due 2023-09-27; ransomware use Unknown

Problem Types: CWE-94

CISA Known Exploited Vulnerability

Vendor	Apache
Product	RocketMQ
Name	Apache RocketMQ Command Execution Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	https://lists.apache.org/thread/1s8j2c8kogthtpv3060yddk03zq0pxyp; https://nvd.nist.gov/vuln/detail/CVE-2023-33246

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Rocketmq	All	All	All	All

References

Reference	Source
lists.apache.org/thread/1s8j2c8kogthtpv3060yddk03zq0pxyp	MISC
oss-security - CVE-2023-37582: Apache RocketMQ: Possible remote code execution when using the update configuration function	MISC
Apache RocketMQ 5.1.0 Arbitrary Code Injection ≈ Packet Storm	MISC
CVE Program record	CVE OR

CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

730868 Apache RocketMQ Remote Code Execution (RCE) Vulnerability

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**